# Retirement of SAS 70 and a new generation of Service Organization Control (SOC) Reports

Presented by:
Nina Currigan, KPMG Advisory Manager
Karen Krebsbach, Ernst & Young Advisory Manager

# With you today

**Nina Currigan**
Advisory Manager
KPMG
Denver, CO
ncurrigan@kpmg.com
303-382-7808

**Karen Krebsbach**
Advisory Manager
Ernst & Young
Denver, CO
Karen.Krebsbach@ey.com
720-931-4475

# Agenda

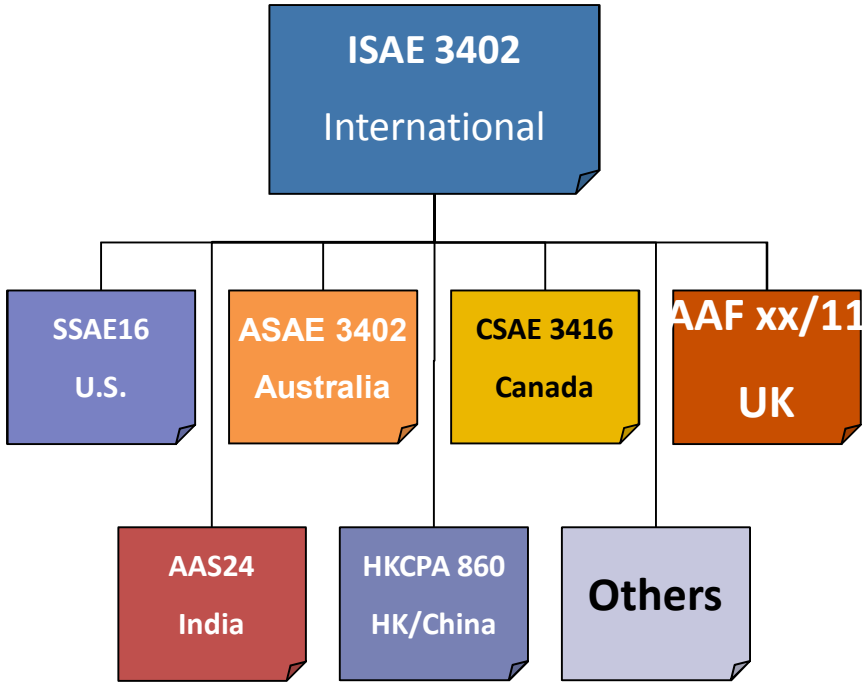
- SAS 70 vs SSAE 16 / ISAE 3402
- Reporting Options
- Impact on Service Organizations
- Impact on User Entities
- Additional reporting options (SOC 2 and SOC 3)
- Resources
- Panel Discussion

# SAS 70 vs SSAE 16 / ISAE 3402

## Historically vs Now

- Historically…


- Now…




ISACA
Trust in, and value from, information systems
Denver Chapter

*Retirement of SAS 70 and a*
*New Generation of Service Organization Control (SOC) Reports*
*April 28, 2011*

# SAS 70 vs SSAE 16 / ISAE 3402

## Key similarities and differences for Service Organizations

| SAS 70 | SSAE 16 / ISAE 3402 |
|---|---|
| Audit Standard | Attestation Standard |
| Management Representation required | Management Representation required |
| Management Assertion NOT required | Management Assertion required |
| No Suitable Criteria Standard | Suitable Criteria Standard |
| Three Opinions | One Opinion |
| Fairness of Presentation as of a point in time | Fairness of Presentation over a period |
| Design as of a point in time | Design over a period |
| Operating Effectiveness over a period | Operating Effectiveness over a period |
| Auditor Requirements limited to testing | Auditor Requirements Expanded |
| No Requirement to disclose use of Internal Audit | Requirement to disclose use of Internal Audit |

# SAS 70 vs SSAE 16 / ISAE 3402

## Key similarities and differences for Subservice Organizations

| SAS 70 | SSAE 16 / ISAE 3402 |
|---|---|
| Carveout and inclusive reporting methods | Carveout and inclusive reporting methods |
| Inclusive method requirements | |
| Management Representation required | Management Representation required |
| Management Assertion NOT required | Management Assertion required |
| Inclusion of COSO elements encouraged | Inclusion of COSO elements required |
| Interaction not required | Acknowledgement required |
| Auditor Requirements limited to testing | Auditor Requirements Expanded |

# Reporting Options

- Consider the users of the report when determining the best reporting option
  - SSAE 16 only report
  - Combined SSAE 16 / ISAE 3402 report

- For other countries, rules may differ
  - Reporting under SSAE 16 may be permissible
  - Reporting under ISAE 3402 only may be permissible

# Impact on Service Organizations

- Management provides a written assertion for inclusion in the report [SSAE 16: 4]
- Management must have a reasonable basis for the assertion [SSAE 16: 9.c.ii]
- That reasonable basis must be based on Suitable Criteria [SSAE 16: 13]

# Impact on Service Organizations

## Suitable Criteria – Fairness of Presentation

Does management's description include all of the following, where applicable:

- The types of services provided including, as appropriate, the classes of transactions processed.
- The procedures, within both automated and manual systems, by which services are provided, including as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities.
- The related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
- How the service organization's system captures and addresses significant events and conditions other than transactions.
- The process used to prepare reports and other information for user entities.
- The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.
- Other aspects of the service organization's control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to the services provided. (Ref: par. A17 and A24)

[SSAE 16: 14]

# Impact on Service Organizations

## Suitable Criteria – Fairness of Presentation

- Does management's description include relevant details of changes to the service organization's system during the period covered by the description?
- Does management's description not omit or distort information relevant to the service organization's system?

[SSAE 16: 14]

# Impact on Service Organizations

## Suitable Criteria – Design

Did management's criteria include the following:

- Identification of the risks that threaten the achievement of the control objectives stated in management's description of its system.
- Identification of controls in management's description of its system that would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

[SSAE 16: 15]

# Impact on Service Organizations

## Suitable Criteria – Operating Effectiveness

Did management's criteria include the following:

- An evaluation of whether the controls were consistently applied as designed throughout the specified period
- An evaluation of whether manual controls were applied by individuals who have the appropriate competence and authority

[SSAE 16: 16]

# Impact on User Entities

- Timing of SSAE 16 – Required for all reports with periods ending on or after June 15, 2011 (early adoption is permitted)
- Understanding management's assertion
- Understanding complementary user entity controls
- Understanding subservice organizations and reporting approach
  - Inclusive
  - Carve-out
- For the most part, users should expect control objectives, control activities and testing to be consistent with that of historical SAS 70
- Users may see changes in scope based on the service organizations re-evaluation of risks, relevance of controls to financial reporting, etc.

# Impact on User Entities

## How to Read a SOC 1 Report

- Review opinion
- Determine whether scope of the report is adequate
- Review complementary user entity controls
  - Determine key vs. non-key
  - Identify existing controls for key complementary user entity controls
  - Document analysis
- Review adequacy of testing by the Service Auditor
- Review exceptions and determine impact
- Consider reviewing in this order:
  - Section I
  - Section III
  - Section II
  - Section IV

# Additional Reporting Options

## Introducing the SOC reports


Reports on Controls at Service Organizations Relevant to Security, Confidentiality, Availability, Processing Integrity, and/or Privacy

SysTrust℠

→ SOC 1 reports

→ SOC 2 reports

→ SOC 3 reports

# Additional Reporting Options

## SOC 2 and SOC 3 reports

- Report subject matter includes areas of internal control outside of financial controls
  - Regulatory compliance (e.g., HIPAA)
  - Operational metrics
- Performed under AT Section 101 (Attest Engagements) of the attestation standards using the Trust Services Criteria
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- US created guidance; designed so it can also be used in other countries

# Additional Reporting Options

## Trust Services Principles

- Security - the system is protected against unauthorized access (both physical and logical)
- Availability - the system is available for operation and use as committed or agreed
- Processing Integrity - system processing is complete, accurate, timely, and authorized
- Confidentiality - information designated as confidential is protected as committed or agreed
- Privacy - personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles GAPP issued by the AICPA and Canadian Institute of Chartered Accountants

** One or more of the principles can be selected for the report **

# Additional Reporting Options

## Trust Services Principles and Criteria

Procedures to address the principles are divided into the following broad categories:

- **Policies** – policies relevant to the principle exist
- **Communications** – policies have been communicated to relevant parties
- **Procedures** – procedures are placed in operation to achieve the objectives defined in the policies
- **Monitoring** – the system is monitored and action is taken to maintain compliance with policies

The standard criterion for each principle are publicly available to readers of the report on AICPA site or in the report

# Additional Reporting Options

## SOC 2 report

- Broader distribution in comparison to SOC 1: existing AND prospective customers, regulators, business partners
- Detailed report format similar to a SOC 1 with Type I or Type II options
- Opinion covers description of system, control design, and control operating effectiveness (for Type II)
- Should not be relied upon for financial statement audit support by user entities

# Additional Reporting Options

## SOC 3 report


- Previous format was a SysTrust report
  - Updated seal for SOC 3

- Same subject matter as a SOC 2 report with key differences:
  - General use report
  - No description of tests and results
  - Opinion covers the management assertion or subject matter of the report (not the description of the system)
  - Seal may be posted on site including a link to the report (if unqualified)

# Additional Reporting Options

## Why SOC 2 / SOC 3 – user entity perspective

- Improve / enable customer oversight of the service organization
- Enhance customer vendor selection and management
- Regulatory or operational compliance
- If a SAS 70 was received in the past, who was relying on it? Will that subject matter be addressed in a SOC 1 considering the focus on financial reporting?

# Additional Reporting Options

## Why SOC 2 / SOC 3 – service organization perspective

- Demonstrate compliance with requirements
- Marketing / competitive edge in RFP processes
- Reduce on-site audits or questionnaires
- Integral piece of the service package provided to customers

# Additional Reporting Options

## Comparing the options

| SOC 1 | SOC 2 or SOC 3 |
|---|---|
| Controls related to financial statements of user entities | Controls related to security, availability, confidentiality, processing integrity, and/or privacy |
| AICPA SSAE 16 standard / IAASB ISAE 3402 standard | AICPA AT 101 |
| Restricted use report (existing user entities and their auditors only) | Wider distribution options (SOC 3 for general / public use) |
| Management identifies control objectives and controls specific to the services covered | Report is based upon the existing Trust Services Principles and Criteria |

# Resources

- www.aicpa.org/soc
- SOC Brochure - Service Organization Controls: Managing Risks by Obtaining a Service Auditor's Report (describes key differences and purposes for SOC 1, SOC 2, and SOC 3) – www.aicpa.org/soc
- www.webtrust.org/ for information about Trust Services Principles and Criteria

Nina Currigan: ncurrigan@kpmg.com

Karen Krebsbach: karen.krebsbach@ey.com